
Entrust®
Securing the Internet
Entrust®
CygnaCom™

Demonstration Components

CygnaCom Software Development Efforts for the Bridge CA Phase II Demonstration

Entrust
CygnaCom™

Bridge CA

- **Initially developed for NIST as a reference implementation of the Minimum Interoperability Specification for PKI Components (MISPC) / 1997-98**
- **Enhanced for Department of Energy 1998-99**
- **Modified for Bridge CA Phase I demonstration 9/99**
  - Crypto changed to use Spyrus LYNKS card
  - Accepts self-signed certificate or file-based CMP request for certification
  - Provides request as either self-signed certificate or PKCS#10 request

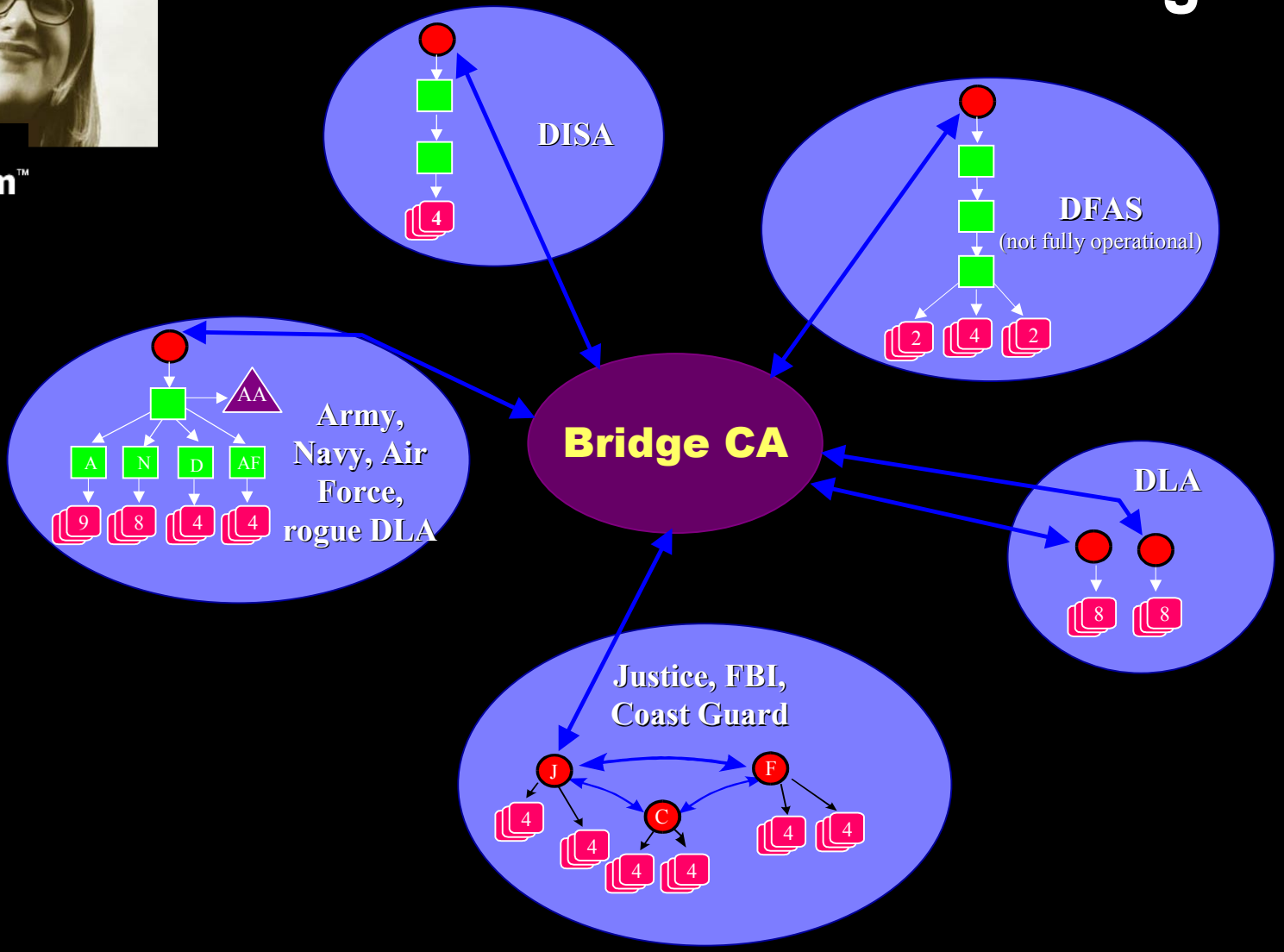
Bridge CA

- **BCA Phase II demonstration required further changes:**
  - Required certificate extensions:
    - Name Constraints
    - Policy Constraints
    - Policy Mapping
  - Cross-algorithm Certificates
  - Standardized key identifier generation

Demonstration Components

Entrust
CygnaCom™

Bridge CA



Certificate Path Development Library

- **The Certificate Path Development library constructs certificate paths in hierarchical or non-hierarchical certificate graphs**
- **It has a number of advantages over existing implementations**
  - Utilizes crossCertificatePair
  - Performs loop detection
  - Caches developed certificate paths
  - Contains many optimizations to help find the best path first

Certificate Path Development Library

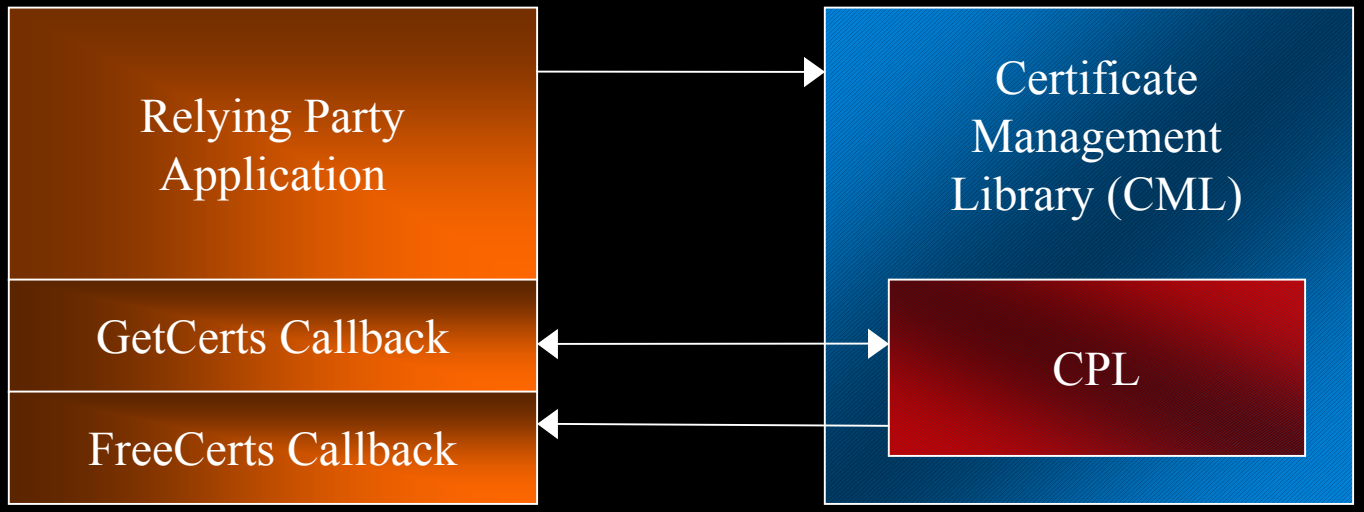
Entrust
CygnaCom™

- **Matching rules filter out unwanted certificates**
  - key usage
  - subject key identifier
  - expired certificates
- **Sorting rules prioritize certificates that are more likely to develop a valid path**
  - RDN components in common with root
  - Consistent algorithm
  - cACertificate over crossCertificate

Certificate Path Development Library

Entrust
CygnaCom™

- **Allows users to provide own Certificate/CRL caching and retrieval mechanisms to avoid reliance on a particular repository**
- **Integrated into CML to replace built-in certificate path development functionality**



Certificate Path Development Library

- **Developed in ANSI C++**
  - Used successfully in Windows 95/98/NT/2000 and Solaris
- **Released by CygnaCom as freeware**
  - v1.31 on CygnaCom website:
    - http://www.cygnacom.com/products
  - v2.0 getting finishing touches; available upon request
- **Integrated into the alpha MailSecure application that was tested in this effort**

VisualSPIF

- Graphical Security Policy Information File (SPIF) editor
- Simplifies use of very complicated structure
- Used by DoD to develop/modify operational SPIFs
- Modified for BCA Phase II Demonstration to allow use of Spyrus LYNKS card, and to read/post SPIFs to/from LDAP directory

Entrust
CygnaCom™

VisualSPIF

- View/Edit classifications

GENSER LIGHT.spf - VisualSPIF

File Edit View Tools Grids Options Help

Classifications
Categories
Tag Sets
Properties
ASN.1 Dump

Add Classification | Edit Classification | Remove Classification

Classification	LACV	Hierarchy Value	Required Categories
UNCLASSIFIED//	1	3	
CONFIDENTIAL//	3	8	onlyOne: NONE [GENSER Security Categories: restricted(1): 3] NOFORN [Genser US Government Categories: restricted(1): 5] onlyOne: GENSER Automatic Declassification Exemptions (Tag set 11 - Tag f AUTOMATIC DECLASSIFICATION EXEMPTIONS: no access controli
SECRET//	4	11	onlyOne: NONE [GENSER Security Categories: restricted(1): 3] NOFORN [Genser US Government Categories: restricted(1): 5] onlyOne: GENSER Automatic Declassification Exemptions (Tag set 11 - Tag f AUTOMATIC DECLASSIFICATION EXEMPTIONS: no access controli
TOP SECRET//	5	14	onlyOne: NONE [GENSER Security Categories: restricted(1): 3] NOFORN [Genser US Government Categories: restricted(1): 5]

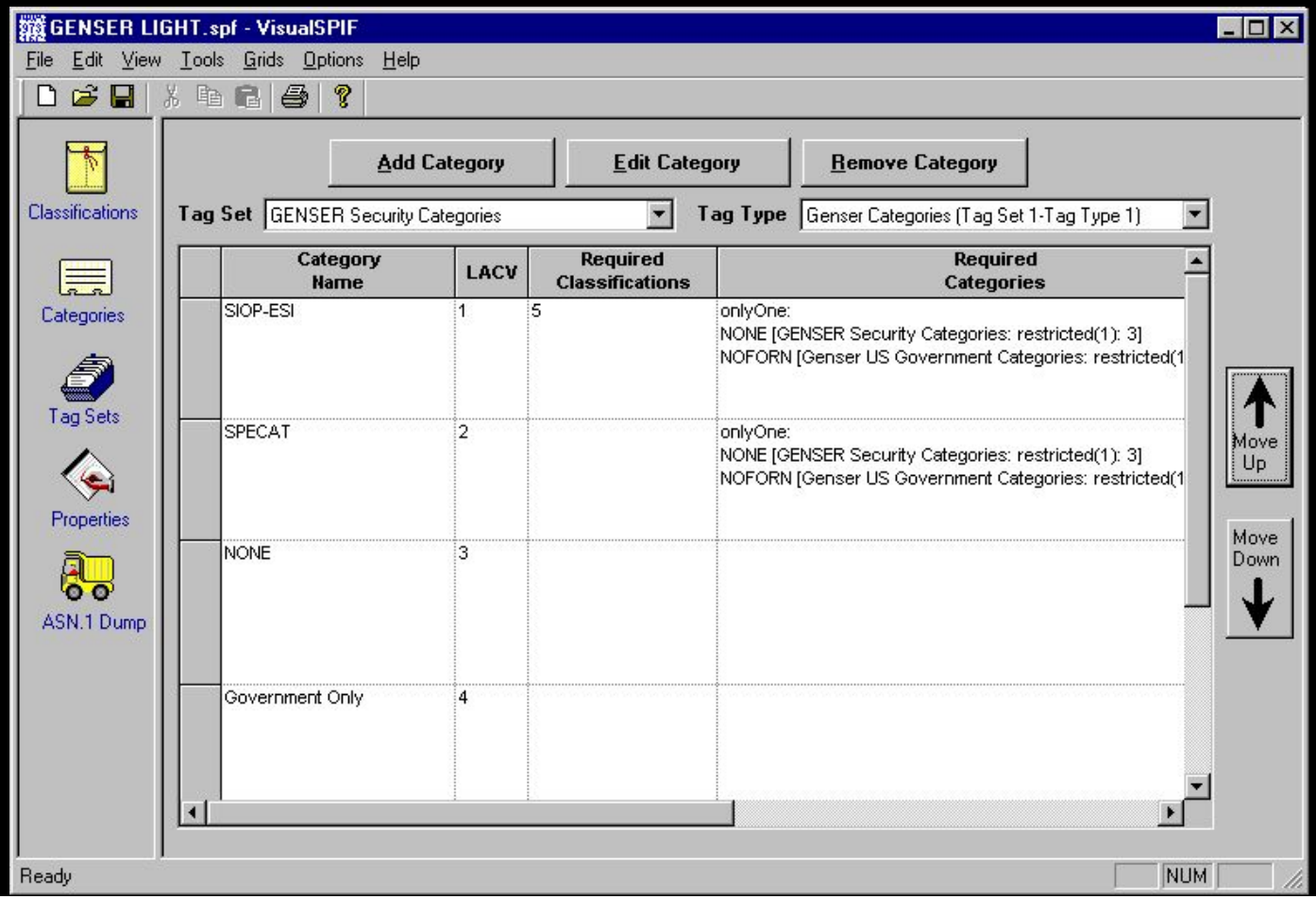
Move Up
Move Down

Ready NUM

Entrust
CygnaCom™

VisualSPIF

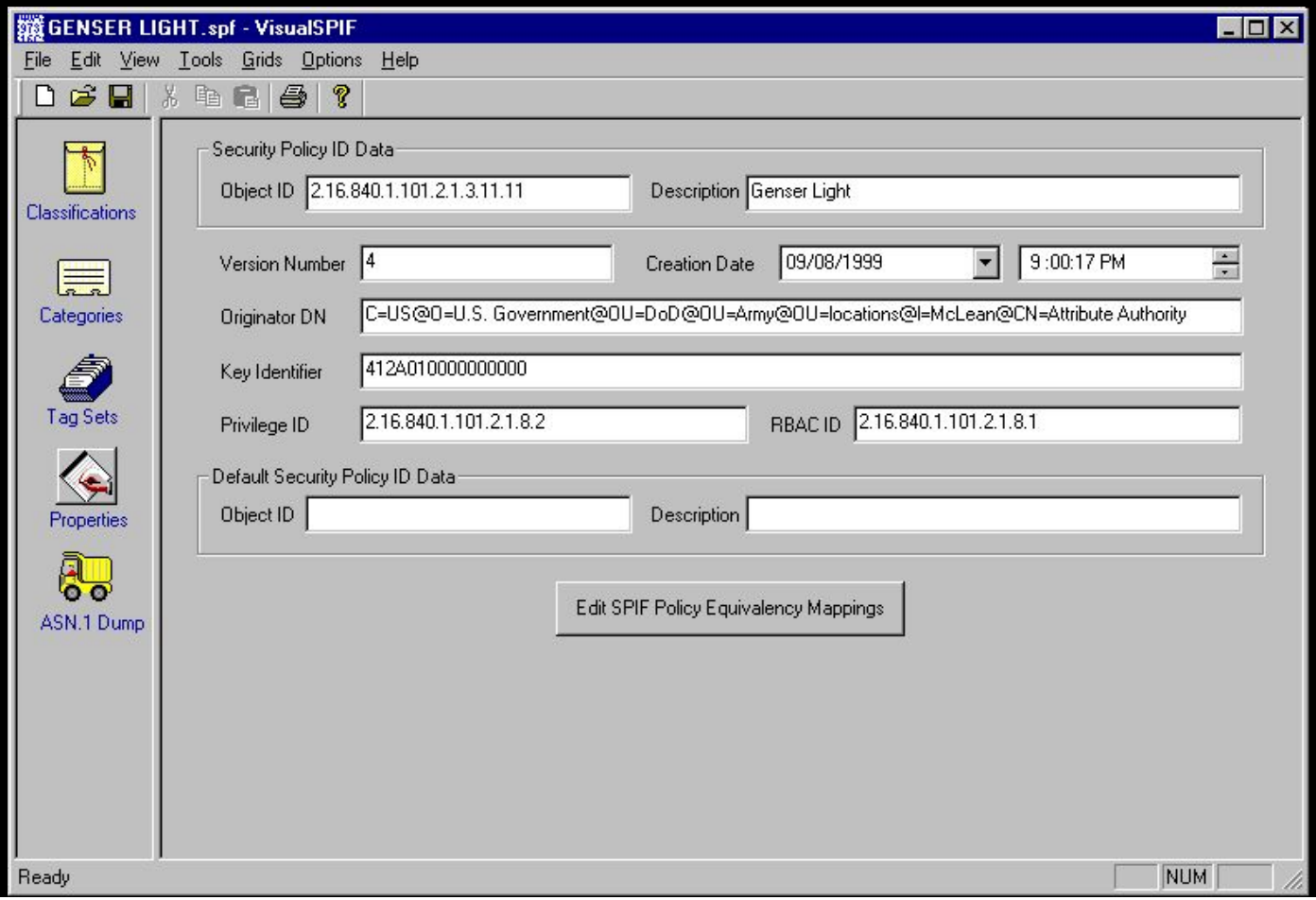
- View/Edit categories



Entrust
CygnaCom™

VisualSPIF

- **View/Edit SPIF Properties**



Entrust
CygnaCom™

VisualSPIF

- View ASN.1 Encoding of SPIF

GENSER LIGHT.spf - VisualSPIF

File Edit View Tools Grids Options Help

Classifications
Categories
Tag Sets
Properties
ASN.1 Dump

```
  0 30 2293: SEQUENCE {
  4 30  168:   SEQUENCE {
  7 02    1:     INTEGER 4
 10 18   15:     GeneralizedTime '199909082100172'
 27 30  135:     SEQUENCE {
 30 31   11:       SET {
 32 30    9:         SEQUENCE {
 34 06    3:           OBJECT IDENTIFIER countryName (2 5 4 6)
 39 13    2:           PrintableString 'US'
                       }
                     }
 43 31   24:       SET {
 45 30   22:         SEQUENCE {
 47 06    3:           OBJECT IDENTIFIER organizationName (2 5 4 10)
 52 13   15:           PrintableString 'U.S. Government'
                       }
                     }
 69 31   12:       SET {
 71 30   10:         SEQUENCE {
 73 06    3:           OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
 78 13    3:           PrintableString 'DoD'
                       }
                     }
 83 31   13:       SET {
 85 30   11:         SEQUENCE {
 87 06    3:           OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
 92 13    4:           PrintableString 'Army'
                       }
                     }
 98 31   18:       SET {
```

Ready NUM

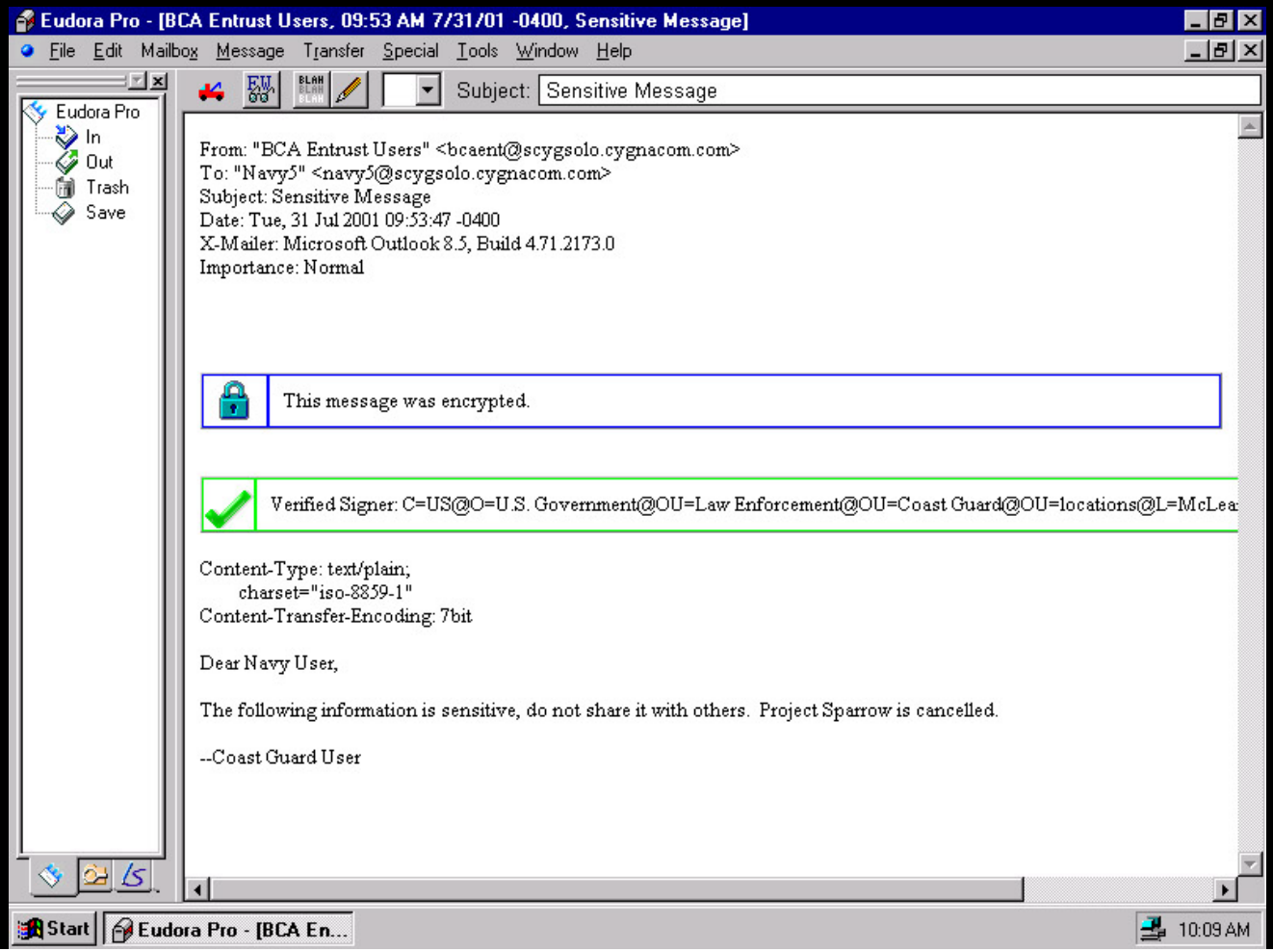
Secure Email Plug-in

- **Developed a plug-in to exercise the features of freeware libraries**
  - Certificate path development in BCA structure **(CPL)**
  - Certificate path validation able to process policies and name constraints **(CML)**
  - S/MIME v3 signing and encryption **(SFL)**
  - Access control using attribute certificates and SPIF **(ACL)**
- **Developed as a plug-in to Qualcomm Eudora**
  - Simplest development interface, exposed all the features we needed

Entrust
CygnaCom™

Secure Email Plug-in

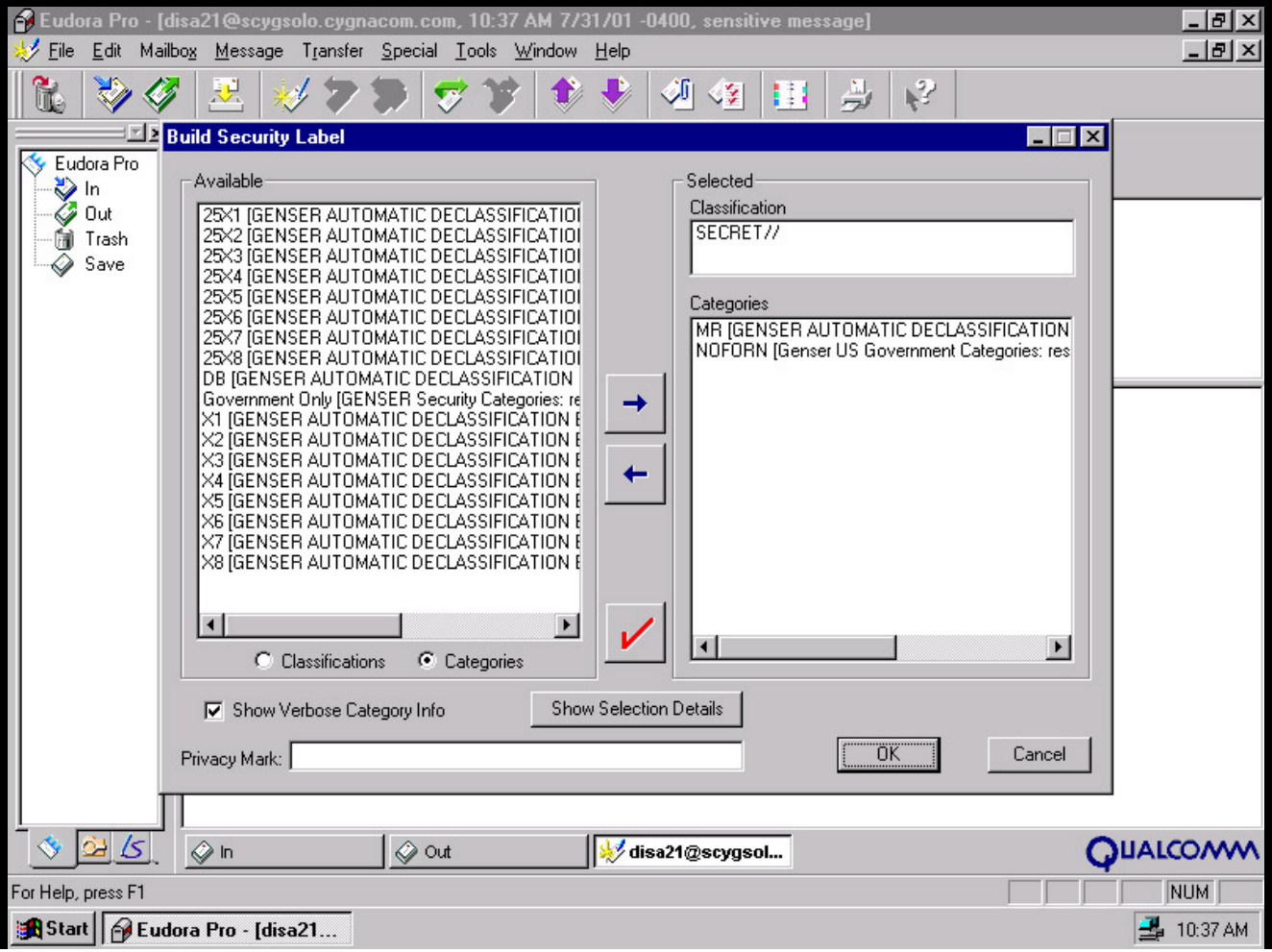
- **Signed and encrypted message after decryption and verification**



Entrust
CygnaCom™

Secure Email Plug-in

- **Choosing a label for a message**



Entrust
CygnaCom™

Secure Email Plug-in

- **Labeled message after verification and processing**

Eudora Pro - [BCA Spyrus Users, 10:38 AM 7/31/01 -0400, sensitive message]

File Edit Mailbox Message Transfer Special Tools Window Help

Eudora Pro
In
Out
Trash
Save
Test Msg

Subject: sensitive message

X-Sender: bcaspy@scygsolo
X-Mailer: QUALCOMM Windows Eudora Pro Version 4.2.0.58
Date: Tue, 31 Jul 2001 10:38:21 -0400
To: disa21@scygsolo.cygnacom.com
From: BCA Spyrus Users <bcatest@sisko.cygnacom.com>
Subject: sensitive message

Label: **Security Label**
Page Top : SECRET// - MR - MR - NOFORN

Verified Signer: C=US@O=U.S. Government@OU=DoD@OU=Navy@OU=locations@L=McLean@CN=Navy User 7

Dear Sir,
Please be advised that U.S. Personnel in your area may be in serious danger. Be careful.

Label: **Security Label**
Page Bottom : SECRET// - MR - MR - NOFORN - NOFORN

In | BCA Spyrus Use... | QUALCOMM

NUM

Start | Eudora Pro - [BCA Sp... | 10:24 AM

Attribute Authority

- **Developed to create, sign, and post attribute certificates for users in the demonstration**
- **User configures database of access rights for all users in system**
- **Attribute authority issues attribute certificates periodically with short lifetime**
  - Configurable; demonstration settings were 2-day lifetime issued every 24 hours
- **Uses SPIF to determine access control rules**
- **Integrates ACL for rule checking and encoding/decoding of attribute certificates**
- **Automatically posts certificates to LDAP directory**

Entrust
CygnaCom™

Attribute Authority

- **User Database**

AttributeAuthority: Manage Users

File Tools View Help

Subject DN	Posted	Expires
CN=Air Force User 1, L=Annapolis Junction	04/24/2001 14:59	10/21/2001 14:58
CN=Air Force User 3, L=Annapolis Junction	04/24/2001 15:01	10/21/2001 15:01
CN=Air Force User 5, L=McLean, OU=locati	04/24/2001 16:52	10/21/2001 16:51
CN=Air Force User 7, L=McLean, OU=locati	04/24/2001 16:52	10/21/2001 16:52
CN=Army User 1, L=Annapolis Junction, OU	04/24/2001 16:53	10/21/2001 16:52
CN=Army User 2, L=Annapolis Junction, OU	04/24/2001 16:54	10/21/2001 16:53
CN=Army User 3, L=Annapolis Junction, OU	04/24/2001 16:54	10/21/2001 16:54
CN=Army User 4, L=Annapolis Junction, OU	04/24/2001 16:55	10/21/2001 16:54
CN=Army User 5, L=McLean, OU=locations,	04/24/2001 16:07	10/21/2001 15:02
CN=Army User 6, L=McLean, OU=locations,	04/24/2001 16:55	10/21/2001 16:55
CN=Army User 7, L=McLean, OU=locations,	04/24/2001 15:03	10/21/2001 15:02
CN=Army User 8, L=McLean, OU=locations,	04/24/2001 16:55	10/21/2001 16:55
CN=Coast Guard 5 User, L=McLean, OU=lo	04/25/2001 15:32	10/22/2001 15:32

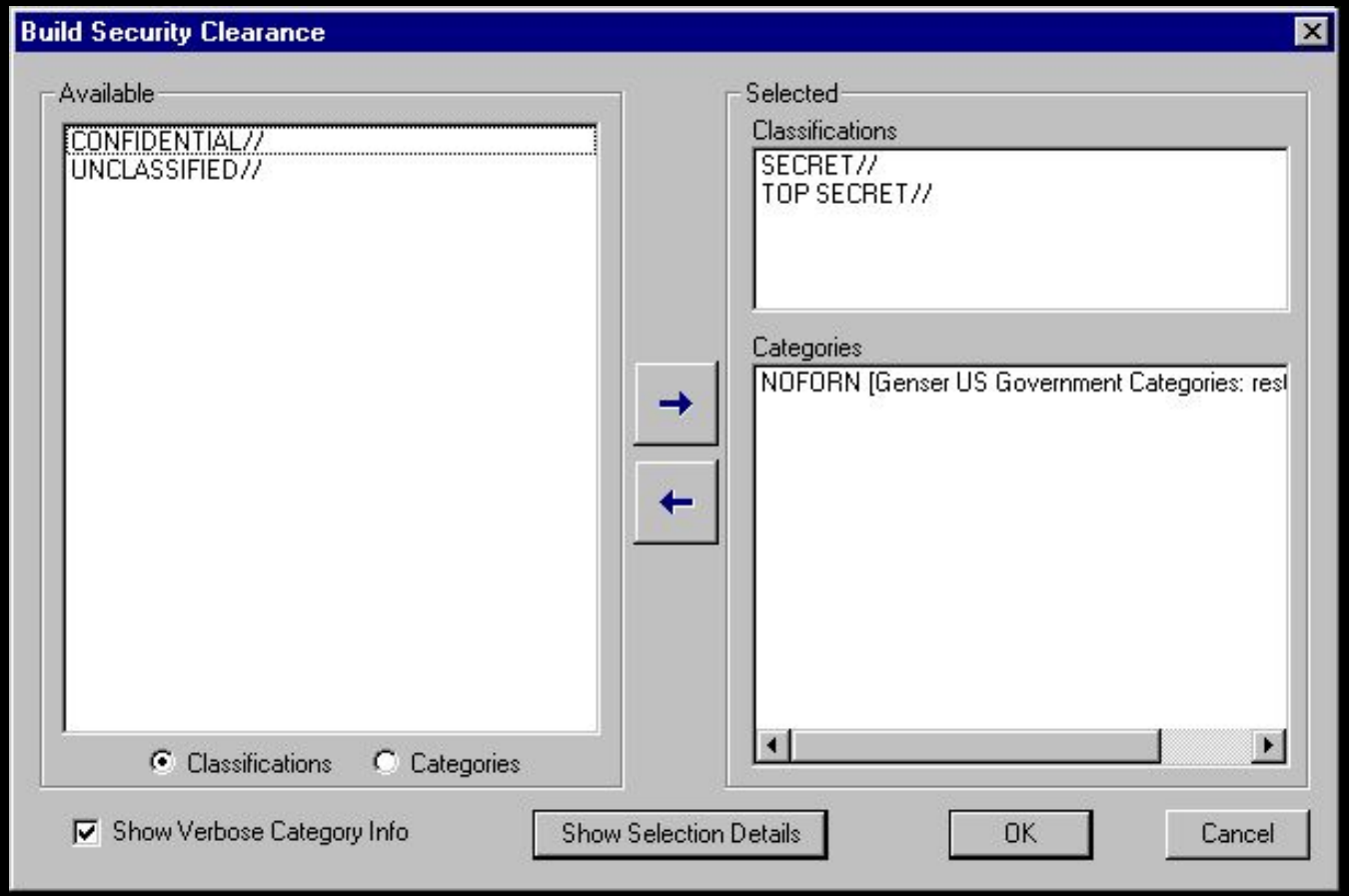
Add User | Remove User | View/Edit Attribute Certificate | Refresh Attribute Certificate

Ready CAP NUM

Entrust
CygnaCom™

Attribute Authority

Choosing User Permissions



Entrust
CygnaCom™

Web Server Plug-in

- Developed to check user authorizations before allowing access to web resources
- Initially developed as a demonstration for DoD using DMS key management certificates containing access control
- This version uses attribute certificates instead of key management certificates
- Integrates CML/CPL/ACL for checking user public key and attribute certificate validity
- Protected pages have a META tag containing the label listing the sensitivity of the information on the page

Entrust
CygnaCom™

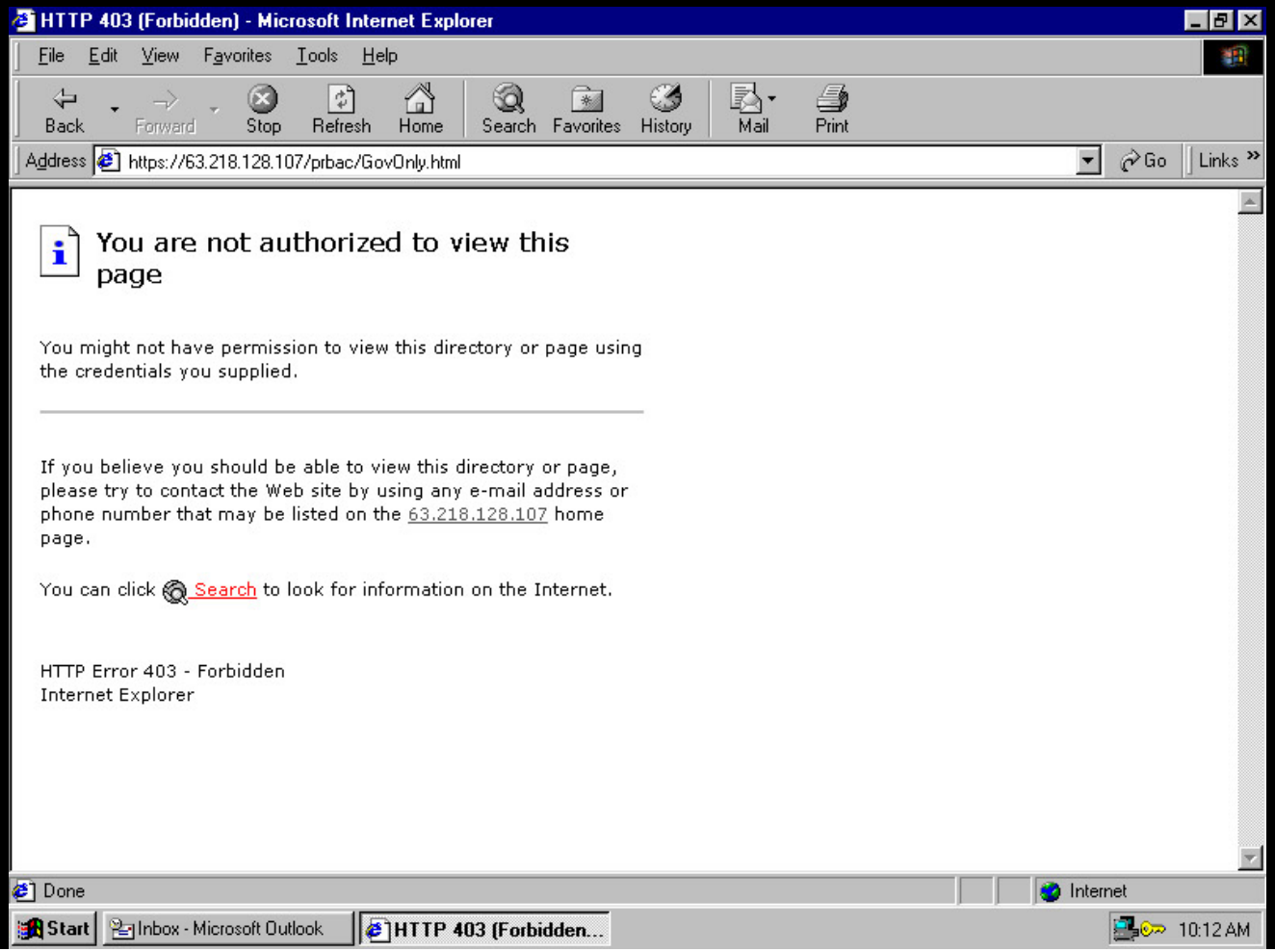
Web Server Plug-in

- **iPlanet web server (out-of-the-box) configured to use SSLv3 mutual authentication in order to obtain client certificate**
  - Web server needed to be configured with every root in our demonstration
    - See technical lessons learned later in this briefing
- **Plug-in checks certificate path and access control, but only on protected pages**
  - Performs no caching to show instant changes in access
- **Generates human-readable label in real time**

Entrust
CygnaCom™

Web Server Plug-in

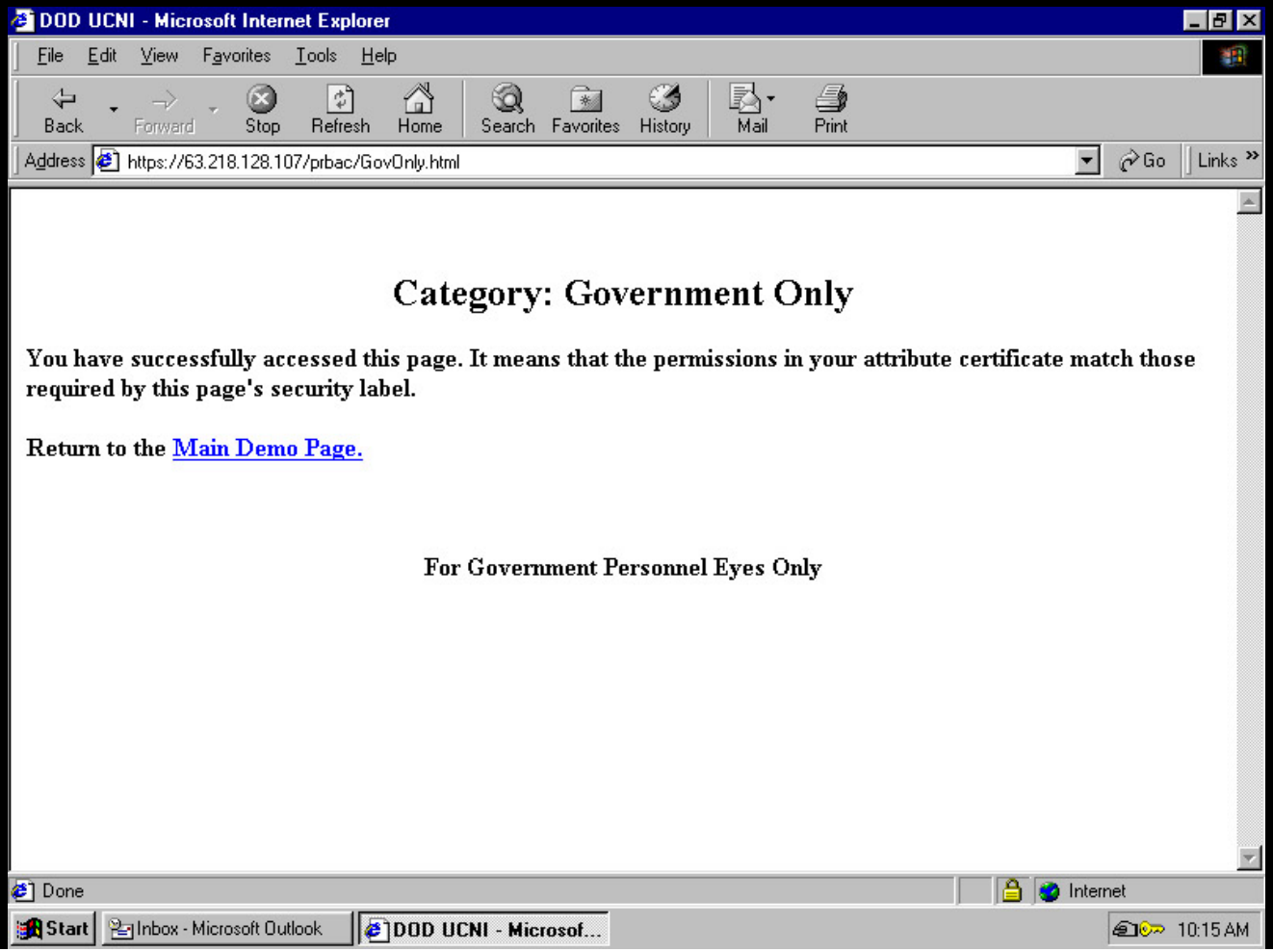
- **Page that cannot be viewed due to insufficient permissions**



Entrust
CygnaCom™

Web Server Plug-in

- **Protected page successfully viewed**



CygnaCom Component Availability

- **BCA**
  - Current version not available; contact NIST for MISPC version
- **CPL**
  - Freely available on website
- **VisualSPIF**
  - Available with DoD and CygnaCom permission
- **Secure Email Plug-in, Attribute Authority, Web Server Plug-in**
  - Available to Government for use/review
  - Will require modifications for operational use

Demonstration Components

Entrust Products used in the Bridge CA Phase II Demonstration

Entrust Authority

- **Entrust/Authority 5.1**
  - Included lesson learned from Phase 1
    - Construction of both forward and reverse elements of cross certificate pair
  - Running on Windows NT 4.0

Entrust Express

- **Entrust/Express 5.1**
  - Express for Outlook used
  - Also available for Groupwise, Notes and Eudora
- **SMIMEv3 Compatible**
  - Commercial 5.1 based upon original Express product which pre-existed SMIMEv3
  - Two Key Pair functionality etc…
  - However needed to update for OID usage and other v3 elements
  - Changes being incorporated to next release of Express for full v3 compliance.

Entrust WebConnector

- **WebConnector is a protocol translator**
  - Entrust/Authority uses PKIX-CMP for advanced Certificate and Key Management features
  - Standard browsers only support PKCS#7/#10 exchanges
  - WebConnector provides the linkage between the two
- **Other Connectors for:**
  - Smart Cards Bulk issuance
  - Mobile Devices
  - SET Devices

Entrust Toolkit

- **Entrust/Toolkits provide high level API to all the key management and cryptographic functions in the Entrust Kernel.**
  - Includes full path discovery and validation
  - Allows use of any X.509 certificate for processing
  - Allows use of a variety of key stores including:
    - Entrust Key Store
    - CAPI Key Store
    - PKCS#12 key Store
  - C, C++, VB, JAVA all available
  - See https://www.entrust.com/developer/software/index.cfm

Entrust Product Availability

- **Just Released Version 6**
  - 6th generation of product
  - Being shipped as of Early July
  - Includes tight Microsoft Integration for CA and Desktop functions
  - And a whole bunch of other stuff
- **More Information at**
  - http://www.entrust.com/authority/index.htm

Demonstration Configuration

How the components were structured for the Bridge CA Phase II Demonstration

Certificate Authorities

- **Bridge CA**
  - Offline; issues CRL with long lifetime
- **"Law Enforcement" domain**
  - Contains three CAs
    - Justice CA
    - FBI CA
    - Coast Guard CA
  - All three CAs cross-certified with each other
  - Online; issues CRLs every 48 hours
- **Justice CA was arbitrarily chosen to cross-certify with Bridge CA**

X.500 Directories

- The “Law Enforcement” CAs have their own directory servers which are set up in chaining relationships to each other
- Since Justice CA cross-certified with the Bridge, the Justice Directory was chosen to perform X.500 chaining with the Bridge Directory
- The Bridge directory is in turn chained to the DoD Border directory

Laboratories

- CygnaCom and Entrust had two laboratories dedicated to the Phase II demonstration effort
- The Entrust lab was dedicated to hosting the online “Law Enforcement” CAs and directories, and provided clients for the PKI.
- The CygnaCom lab was the site of much of the system testing and integration that went on as a part of the effort. All clients and access control-related servers were hosted here.

Entrust Lab Configuration

- CA - Justice
- Directory

To DOD Bridge via Internet

- CA - USCG
- Directory

- CA - FBI
- Directory

X.500 Chaining

Local Network

- Entelligence
- Express

- AutoRA
- WebConector

- Entelligence
- Express

CygnaCom Lab Configuration

Entrust
CygnaCom™

Internet

SMTP and LDAP

- AC Enabled Web Server
- Bridge CA
- Attribute Authority
- VisualSPIF
- Mail Server
- Proxy Server

- Entrust Client
  - Outlook w/Express
- Spyrus Client
  - Eudora w/Plug-in
- Baltimore Client
  - Outlook w/MailSecure
- Motorola Client
  - Eudora w/Plug-in

Phase II Demonstrations

- **Held at CygnaCom and Getronics Facilities in five parts**
  - Technical discussion of Bridge CA Interoperability (conference room)
  - Demonstrations of secure messaging (lab)
  - Technical discussion of Access Control (conference room)
  - Demonstrations of access control (lab)
  - Conclusion/Wrap-up/Questions (conference room)
- **Generally under 3 hours with breaks**
- **Limited space that fills quickly; sign up soon!**

Technical Lessons Learned

- **Quite a number of lessons were learned during the engineering and testing of this demonstration**
  - Not all the lessons were technical in nature!
- **Feedback from the testing was fed to product development for the various products**
- **Most of the problems encountered have already been fixed for the next release of products**

Technical Lessons Learned Directory Chaining and Time

- **We encountered many problems with directory chaining that were related to the time synchronization of the machines that were chained.**
  - Some errors due to improper time zone calculations
  - Other clocks were just off due to floating time
- **Errors encountered were unpredictable erratic responses from server accepting chained request**
  - Time being off a little caused different results to be returned at different times
  - Time being off a lot (due to timezone problems) led to no results
- **Lesson: Plan to synchronize time between directories. NIST provides networked time service.**

Technical Lessons Learned
Key Identifier Calculations

- **If Agency A issued all its certificates with the authority key identifier extension containing a key value X, the Bridge CA must issue its cross-certificate with Agency A containing nothing other than X in the subject key identifier**
  - This is because processing systems often use the key identifier as a factor to rule out certificates when building paths.
- **Standards give guidance on how to generate values**
  - Guidance is a recommendation, not a must-implement
  - Not all products are flexible in the generation of these values
- **Lesson: Be aware that AKID/SKID values must match in cross-certificates, or processing systems will not find/recognize/validate paths**

Technical Lessons Learned Web Servers and Path Building

- **Generally speaking, web servers are not equipped to build paths**
  - Unless strict hierarchy
  - And client provides certificates up to a trust root in request
- **If a web server is configured to trust an agency CA, that may not be enough to trust users in other agencies.**
- **Lesson: Manually add all known cross-certificates and intermediate certificates to web server trust list in addition to local agency root CA. Push web server vendors to include this ability in future versions.**

Bridge CA Enabling

How Entrust and CygnaCom can enable your organization to work with the Federal Bridge CA

Labor Efforts

- **During Phase I demonstration, I outlined basic levels of effort required for development of plug-ins using freeware libraries and Entrust Toolkit**
- **A similar analysis today is less valuable now because**
  - We did not develop a plug-in using Entrust Toolkit for Phase II
  - I work at Entrust-CygnaCom
- **Basic points remain the same though**
  - Freeware libraries are more low-level/Entrust toolkit is higher level
  - Entrust toolkit allows faster development of more complicated processes, at the cost of reduced flexibility and opaque source code

Entrust
CygnaCom™

Labor Efforts

- The chart below approximates some of the comparable effort levels from our experience

	Freeware Libraries (CPL/CML/SFL/ACL)	Entrust Toolkit
Certificate Path Building	easy	easy
Certificate Path Validation	medium	easy
Basic crypto ops. (sign/encrypt...)	easy	easy
Create PKCS 7 signed message	medium	easy
Create PKCS 7 sign/enc with attributes	hard	not available (yet)
Attribute certificate based access control	medium	not available

Using Entrust Products with Entrust PKIs for BCA compatibility

Entrust
Securing the Internet

- This is easy...

Using Entrust Products with non-Entrust PKIs for BCA compatibility

Entrust
Securing the Internet

- Entrust Toolkits provide full path discovery and validation
- Entrust Toolkits can use other key stores and can process any X.509 certificate
- Allows use of Entrust Crypto engines to integrate into any application that needs to perform the path validations required by the Bridge using any CA.

We Can Help!

Entrust CygnaCom™

- **CygnaCom, as a division of Entrust Professional Services, is already assisting a number of agencies and organizations preparing to interoperate with the Federal Bridge CA.**
  - CP/CPS development and review
  - PKI Installation and Configuration
  - Directory shadowing/Border directory configuration
  - …and much more!

Entrust Securing the Internet

- **Entrust Authority, Entelligence, and Express are Bridge-CA capable today**

Questions?

Contact Information

Peter Hesse, Manager of Cryptographic Software Development, Entrust CygnaCom

pmhesse@cygnacom.com

(703) 270-3523

Gary Moore, Senior Technical Advisor, Entrust Federal

Gary.Moore@entrust.com

(703) 269-2025


Entrust®
Securing the Internet
Entrust®
CygnaCom™